

ПРОЦЕС НАКЛАДЕННЯ ЕЛЕКТРОННОГО ПІДПISУ

Використання електронного підпису є обов'язковою умовою під час подання тендерної пропозиції та при публікації річних планів та закупівель.

Удосконалений електронний підпис (УЕП) – це підпис, що представляє собою матрицю поєднання електронних даних власника, шляхом криптографічного поєднання файлу УЕП з особистим ключем, що безпосередньо пов'язаний з особою, яка підписує документ. Може зберігатися на будь-якому файловому носії, а тому є менш захищеним, ніж КЕП.

Кваліфікований електронний підпис (КЕП) – це підпис, юридично рівнозначний ручному, що базується на кваліфікованому сертифікаті відкритого ключа. Він є найбільш захищеним видом електронного підпису, оскільки зберігається на спеціальному носії інформації - токени або у спеціальному захищеному хмарному сховищі.

Де отримати КЕП/УЕП?

Файл електронного підпису можна отримати, звернувшись до акредитованого центру сертифікації ключів (АЦСК). Перелік чинних АЦСК доступний на сайті майданчика за посиланням: <https://tender.uub.com.ua/page/acsk>

Як накласти КЕП/УЕП?

Для накладення кваліфікованого або удосконаленого електронного підпису (КЕП/УЕП) необхідно скористатися завантаженим віджетом електронного підпису. У віджеті потрібно обрати відповідний тип підпису:

- «Електронний підпис» — для використання КЕП або УЕП, що зберігається на токени, файловому носії або у хмарному середовищі;
- «Дія.Підпис-UA» — для підпису документів за допомогою мобільного застосунку «Дія».

Електронний підпис

×

Зчитайте ключ

Електронного підпису →

Дія.Підпис - UA →

Версія від 2025.02.05 13:00

Закрити

Після завантаження криптографічної бібліотеки, обравши тип підпису «Електронний підпис», необхідно здійснити вибір типу носія особистого ключа. Доступні такі варіанти:

- **Файловий** — ключ зберігається у вигляді файлу на комп'ютері або іншому файловому носії;
- **Токен** — ключ зберігається на захищеному апаратному пристрої (токені);
- **Хмарний** — ключ розміщується у захищеному хмарному середовищі.

Електронний підпис

Крок 1 з 2

Зчитайте ключ

Файловий Токен Хмарний

Накладення електронного підпису з файлового носія

Після вибору типу носія «Файловий», необхідно виконати такі дії:

1. **Оберіть кваліфікованого надавача електронних довірчих послуг** зі списку;
2. **Завантажте файл особистого ключа** (зазвичай має розширення *.dat або *.zs2);
3. **Введіть пароль до особистого ключа**, встановлений під час його генерації.

Електронний підпис

Кваліфікований надавач електронних довірчих послуг

КНЕДП ТОВ "Центр сертифікації ключів "Україна"

CERTKEY_PERSONAL_KEY_10210000001.ZS2

[Змінити](#)

Пароль захисту ключа

.....

Назад Зчитати

Закрити

Після заповнення всіх необхідних параметрів (вибору надавача послуг, завантаження файлу ключа та введення пароля), слід натиснути кнопку «**Зчитати**». Після успішного зчитування даних відобразиться інформація про підписанта. Для завершення процедури натисніть кнопку «**Далі**» і електронний підпис буде накладено на документ.

Після успішного підписання з'явиться повідомлення: «**Кваліфікований електронний підпис накладено**».

Накладення електронного підпису **з токена**

Після вибору типу носія «Токен» у віджеті електронного підпису, виконайте наступні дії:

1. **Оберіть кваліфікованого надавача електронних довірчих послуг** зі списку.
2. **Оберіть токен зі списку підключених пристроїв** (зазвичай відображається автоматично після вставлення токена у USB-порт).
3. **Введіть PIN-код** до особистого ключа, який зберігається на токені.

Після введення всіх параметрів натисніть кнопку «Зчитати». Після зчитування ключа на екрані з'явиться інформація про підписанта. Для завершення процесу натисніть кнопку «Далі» і електронний підпис буде накладено на документ.

Після успішного підписання з'явиться повідомлення: «Кваліфікований електронний підпис накладено».

Накладення хмарного електронного підпису відбувається аналогічно до підпису з файлового носія та токена.

Процедура накладення підпису за допомогою «Дія.Підпис-UA»

1. Для зчитування QR-коду необхідно авторизуватися в застосунку «Дія».
2. На головному екрані порталу оберіть параметр «Сканувати QR-код» у верхньому лівому куті та виконайте сканування згенерованого системою QR-коду.
3. Після сканування на екрані застосунку з'явиться запит на підписання документа через «Дія.Підпис». Натисніть кнопку «Підписати».
4. Наступний крок – перевірка особи за фото. Необхідні дії відображатимуться одразу на порталі. Для успішного підтвердження особи слід дотримуватися рекомендацій, що з'являються.
5. Після успішної ідентифікації у застосунку з'явиться відповідне повідомлення.
6. Введіть **PIN-код** для «Дія.Підпису».
7. На електронному майданчику у вікні накладення підпису відобразяться дані особи, чий підпис буде накладено, а також файл підпису з розширенням **.cer**.
8. Для завершення процесу накладення підпису натисніть кнопку «Далі».

Закрити

Після виконання цих дій електронний підпис буде накладено. Файл електронного підпису матиме формат **.ps7**.